THE UNIVERSITY OF TENNESSEE HEALTH SCIENCE CENTER

| UT Health Science Center:<br>IT0003-HSC-A.01 Information Security Roles and Responsibilities | |
|---|---|
| **Version 4** | **Effective Date: 09/30/2017** |

| | |
|---|---|
| Responsible Office: Office of Cybersecurity | Last Review: 03/01/2025<br>Next Review: 03/01/2027 |
| Contact: Chris Madeksho | Phone: 901.448.1579<br>Email: mmadeksh@uthsc.edu |

## Purpose

To define the Roles and Responsibilities of all members of the University of Tennessee Health Science Center (UTHSC) Community essential to implementing the UTHSC Information Security Program.

## Scope

All members of the UTHSC Community are subject to the UTHSC Information Security Program.

## Responsibilities

Responsibilities are defined in the Practice section.

## Practice

1. In addition to the responsibilities outlined in IT0003-HSC-A-UTHSC Information Security Program Strategy, the UTHSC Information Security Program identifies the following Roles and Responsibilities:
   a. **UTHSC Office of Cybersecurity**: a group of UTHSC employees assigned to the implementation of the UTHSC Information Security Program. Specific responsibilities include:
      i. Preserve the availability, integrity, and confidentiality of information through the recommendation of the implementation of reasonable and appropriate safeguards and controls following the Center for Internet Security (CIS).
      ii. Develop, implement, and maintain information security standards, practices, and procedures
      iii. Guide and recommend effective information security processes and practices
      iv. Analyze information security risk. Recommend and implement administrative, technical, and operational safeguards toward mitigation/remediation

v. Monitoring of security compliance with internal and external requirements
vi. Provide Information Security awareness training per IT0014-HSC-A-Security Awareness Training Management
vii. Timely response to, and management of, security events and incidents per IT0017-HSC-A-Security Incident Response
viii. Response to reporting requirements
ix. Effective communications

b. **Data Owner**: a senior-level individual (or their documented delegate) overseeing and maintaining UTHSC Data or Information. Specific responsibilities include:
   i. Appropriately categorize UTHSC Data or Information per IT0005-HSC-A-Data & System Categorization
   ii. Assign day-to-day administrative and operational responsibilities to both Data Custodians for UTHSC Data or Information and Application Owners for application(s) maintaining UTHSC Data or Information.
   iii. Approving standards, practices, and procedures related to day-to-day administrative and operational management of UTHSC Data or Information and application(s) maintaining UTHSC Data or Information.
   iv. Determining the appropriate criteria for obtaining access to UTHSC Data or Information and application(s) maintaining UTHSC Data or Information.
   v. Define reasonable and appropriate security controls for the protection of the confidentiality, integrity, and availability of UTHSC Data or Information
   vi. Ensure that Data Custodians implement the defined security controls
   vii. Defining risk tolerance and accepting or rejecting risk related to security threats that impact the confidentiality, integrity, and availability of UTHSC Data or Information

c. **Data Custodian:** a UTHSC employee who has administrative and/or operational responsibility over UTHSC data or Information. Specific responsibilities include:
   i. Implement appropriate physical and technical safeguards to protect the confidentiality, integrity, and availability of UTHSC Data or Information
   ii. Provision and de-provision access to UTHSC Data or Information as authorized by the Data Owner

iii. Understand and report on how UTHSC Data or Information are stored, processed, and transmitted by the University and by third-party entities
iv. Document and disseminate administrative and operational procedures to ensure consistent storage, processing, and transmission of UTHSC Data or Information
v. Understand and report on security risks and how security risks impact the confidentiality, integrity, and availability of UTHSC Data or Information

d. **System or Application owner**: a UTHSC employee or group of employees with the responsibility to ensure that the program or programs, that make up the system or application, accomplish the specified objective or set of user requirements established for that application. Specific responsibilities include:
   i. Responsible for the specific service or application.
   ii. Accountable for incidents, problems, and changes that impact the service or application
   iii. Implement appropriate physical and technical safeguards to protect the confidentiality, integrity, and availability of UTHSC Data or Information supported by the application.
   iv. Assign and modify users to roles in the application based on need-to-know and least privilege.

e. **Users:** any member of the UTHSC Community authorized to access UTHSC IT Resources. Specific responsibilities include:
   i. Adhere to UTHSC Information Security policies, standards, practices, processes, guidelines, and procedures
   ii. Maintain the security, confidentiality, integrity, and availability of data and information the UTHSC creates, acquires, maintains, and distributes in various forms.
   iii. Report violations of the UTHSC Information Security Program per IT0003-HSC-A.003-Information Security Violations

## Policy History

| Version # | Effective Date |
|---|---|
| 1 | 09/30/2017 |
| 2 | 03/30/2020 |
| 3 | 03/01/2025 – new naming convention |

# References

1. IT0002-Acceptable Use of Information Technology Resources
2. IT0003-Information Technology Security Program Strategy
3. IT0014-Information Technology Security Awareness Training Management
4. IT0002-HSC-A.03-Information Security Violations
5. IT0003-HSC-A-UTHSC Information Security Program Strategy
6. IT0005-HSC-A-Data & System Categorization
7. IT0014-HSC-A-Security Awareness Training Management
8. IT0017-HSC-A-Security Information Response